AUSTRALIA

AU 00/01081



**Patent Office**
**Canberra**

I, LEANNE MYNOTT, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PQ2737 for a patent by ACCUDENT PTY LTD filed on 08 September 1999.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Tenth day of October 2000

LEANNE MYNOTT
TEAM LEADER EXAMINATION
SUPPORT AND SALES

**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

P/00/009
Regulation 3.2

AUSTRALIA

*Patents Act 1990*

# PROVISIONAL SPECIFICATION

Invention Title: "DOCUMENT AUTHENTICATION METHOD AND APPARATUS"

The invention is described in the following statement:

THIS INVENTION relates to a document authentication method and apparatus.

The invention is particularly suitable for, but not limited to, validation of financial instruments, including cash (ie., bank notes), personal cheques, traveller's cheques, credit cards, debit cards and the like.

The invention is also particularly suitable for, but not limited to, the validation of legal instruments such as letters, agreements, licences, bills, and copies (eg., photocopies) thereof.

The counterfeiting of documents, particularly currency, has been a major problem for the authorities for many years. Money issuing authorities (eg., Reserve banks or mints) have adopted many different methods in an attempt to overcome or minimise counterfeiting of currency and other financial documents, and examples have included features or indicia such as watermarks and holograms. Examples of papers discussing such matters include (1) "Spacial Logic Algorithms Using Basic Morphological, Anologic CNN Operations" (Zarande et al) in "The Proceedings of the 1994 Third IEEE International Workshop on Cellular Neural Networks and their Applications", Rome, Italy, published in the "International Journal of Circuit Theory and Applications" v 24 n 3 May-Jun 1996, pages 283-300; (2) "Development of Embossed Holograms" (Haines) in "Proceedings of SPIE - The International Society for Optical

Engineering", v 2652, 1996, Society of Photo-Optical Instrumentation Engineers, Bellingham, WA, United States of America, pages 45-52; (3) "Performance of Diffraction Grating on a Banknote - The Experience with the Australian Commemorative Note" (Hardwick) in "Proceedings of SPIE - The International Society for Optical Engineering", v 1210, published by The International Society for Optical Engineering, Bellingham, WA, United States of America, pages 20-26; (4) "Optically Variable Devices for use on Bank Notes" (Rolfe) in "Proceedings of SPIE - The International Society for Optical Engineering" v 1210, published by the International Society for Optical Engineering, Bellingham, WA, United States of America, pages 14-19; (5) "Evaluation of Security Features for new U.S. Currency" (Church et al) in "Proceedings of SPIE - The International Society for Optical Engineering", v 2659, 1996, Society of Photo Optical Instrumentation Engineers, Bellingham, WA, United States of America, pages 28-36.

Whilst such authentication features or indicia can be placed in bank notes, currency or other financial or legal documents, there is a need for financial or legal instruments bearing such indicia, to be rapidly and accurately-identified and authenticated.

It is an object of the present invention to provide a method where a document (eg., a financial or legal instrument, as hereinbefore described), can be authenticated as either valid, or

identified as invalid or counterfeit.

It is a preferred object that the method can be carried out rapidly and accurately.

It is a further preferred object to provide a method which requires minimal hardware requirements.

It is a still further preferred object to provide apparatus for carrying out the method.

Other preferred objects will become apparent from the following description.

In one aspect, the present invention resides in a method for authenticating a document (including, eg., a financial or legal instrument as hereinbefore described) including the steps of:

a) scanning the document for one or more identifying features and/or indicia;

b) comparing the scanned features/indicia against stored information in a database identifying the features/indicia as authentic or otherwise; and

c) transmitting a signal confirming whether or not the document is authentic or otherwise.

Preferably, the features/indicia scanned include watermarks, holograms, serial numbers, words, devices, colours (eg., patterns, combinations) or other features or indicia printed on, embossed into, incorporated in, or otherwise forming part of, the

document.

Preferably, the database contains one or more features/indicia for comparison by which the authentication of the document may be determined. The document may be authenticated when the features/indicia scanned match the criteria of one or more (but preferably a plurality) of identification components stored in the database.

Preferably, when a document is established to be authentic or otherwise, the signal is transmitted to the location at which the document is scanned to indicate whether or not the document is authentic or otherwise.

In a second aspect, the present invention resides in apparatus for authenticating a document (eg., a financial or legal document as hereinbefore described) including:

a terminal operable to scan one or more identifying features or indicia of the document;

a database containing one or more stored identifying features indicative of whether or not the document is authentic or otherwise;

comparator means to compare the scanned features/indicia with the stored identifying features;

transmission means interconnecting the scanning means and the comparator means; and

indicator means operable to receive a signal from the comparator means to indicate whether or not the document is authentic or otherwise.

Preferably, the indicator means is provided on the terminal.

Preferably, the terminal includes scanning means operable to scan the scanned features/indicia hereinbefore described and means to transport the document past the scanning means.

The scanning means may incorporate one or more scanning heads, each operable to scan one or more features/indicia on the documents.

The database may be provided on the central computer which incorporates the comparator means.

The transmission means may incorporate any suitable communication means, eg., telephony, wireless, infra-red, hardware or the like.

In a third aspect, the present invention resides in an apparatus, as described above, where the scanning means is a scanning head passed over the documents (eg., by hand).

In a fourth aspect, the present invention resides in an apparatus for authenticating a document (eg., a financial or legal instrument) including;

a receptacle to receive the document;

means to scan the document as the document enters the receptacle;

data transfer means to transfer scanned data from the scanning means;

and card means operable to receive the data; so arranged that:

the document can only be released from the receptacle when the card means is placed in, or read by, a card reader associated with the receptacle.

To enable the invention to be fully understood, preferred embodiments will now be described with reference to the accompanying drawings, in which:

FIG. 1 is a schematic circuit diagram of a first embodiment;

FIG. 2 is a front view of a terminal for the first embodiment.

In one embodiment (see FIGS. 1 and 2), the system consists of an end user terminal 10 (with a document scanner 11 and end user connector 12) connected to a main computer 20 centre that has a resident database. The database structure is to be hereinafter described.

The end user terminal 10 can be configured in several different ways. This can be a desktop stand-alone device that is

possible, as one application that will enable the operator to be away from the network connection. Another configuration of the end user terminal 10 will be the integration of the terminal into a major piece of business equipment.

The end user terminal document scanner 11 consists of a motorised note tray 110 that is used to draw the note (or document) into and through the terminal. The note is passed through a scanning head. The scanning head is doubled to ensure the note can be read no matter which way the note is inserted. The scanning head contains a number of integrated components, which allow the note to be scanned in several ways. Incorporated in the terminal is an information processing unit. The information is passed through a line terminal device 30 that is appropriate to the type of institution where the equipment is installed.

The tray for the terminal unit 11 is a motorised tray that allows the note to be pulled through the scanning heads at, preferably, a constant velocity. The motor drive for the tray can be preferably set to an almost infinite number of speeds. The motor control unit is integrated into the information processing unit and relies upon an analog control mechanism. The type of currency used, the level of identification required and the need for extra analysis can determine the motor control output.

The scanning unit consists of two identical scanning

heads, one on each side of the tray. The scanning head may consist of a normal scanning head with a calibrateable daylight light source and an integrated circuit embedded into the head to control the colour analysis process. The scanner may be commercially available and the specification will depend upon the ultimate requirement of the colour analysis unit. The output of the scanning heads is fed to the information processing unit where the information is filtered and processed.

The information processing unit (IPU) consists of the main processing unit for the information coming from the scanning unit, an upgradeable memory module and a ROM. All of the software for the terminal unit and the network interface unit is embedded in the ROM. The embedding of the software in the ROM assists in the maintenance of security of the information and to prevent tampering. Within the IPU, a security controller is used to monitor the integrity of the unit by monitoring a system of electronic locks and seals throughout the system. Should the integrity of the system be breached, the unit will transmit a security alarm to the network control site.

For applications that take the user away from the normal fixed terminal, a portable unit (in a second embodiment) will allow the scanning of discrete amounts of information from a note or other instrument. The portable unit scans the area by the user moving the

device over the target area in a constant motion. The information is stored in the unit and compared initially against any information held within the onboard memory. The device can have information downloaded from the system and will normally be used as a first level device used to identify notes or other instruments that require further detailed investigation.

The unit consists of a small scanning head with an integrated light source. The information from the scanning head is fed into a cut-down version of the IPU. The portable device contains a cut-down version of the colour analysis circuitry and used to do preliminary analysis of a designated area on the note. The IPU includes solid state memory that allows the storage of the information gathered from the scan. This information is processed and compared with the information held in memory within the device. Output to the operator is in the form of three lights. "Green" for "passed", "yellow" for "unknown" and "red" for a note that is found to match a number in the memory and requires confiscation or other action as appropriate. (With a yellow light, the note may require manual checking for authenticity/damage.)

The terminal unit can be integrated into almost all money handling machines and processors. These include all types and models of cash draws and totalisers, all money drop boxes, and the units can also be integrated into most secure money safes. The

advantage of the system for money storage is that all of the notes and instruments in the cash storage device can be itemised and accounted for.

The terminal equipment can be locationally separate due to the modular design of the terminal unit. This configuration is ideal where the system is located in an area that needs to remove large holdings of cash from close proximity of the public interface.

The terminal unit can be upgraded in steps to include an integrated EFTPOS terminal, allow for the printing of microdot security devices, validation of magnetic swipe cards and smart cards, the automatic compilation of foreign currency and the instant conversion of foreign currency in real time when connected to the international network. Supporting the system can be an add-on system that will allow individuals and companies to print their own cheques from their account and incorporate a number of hidden security features that will be able to be detected through the terminal. These security features may be a mixture of colour and position controlled by a secret embedded algorithm.

The system employs a large distributed database. The database (for, eg., bank notes) may contain bank note numbers/types and files that correspond to its colour analysis profile. This profile is reduced to a number through the use of an algorithm that is a part of the colour analysis system.

When a note or other instrument is fed into the terminal unit (OTU), the embedded software first determines the denomination of the note through the first output of the colour analysis unit. The note is then scanned and the information is passed to the information processing unit within the OTU. The IU resolves the serial number of the note and requests the note file from the central server unit. When this information is received by the OTU, the serial numbers are compared and all of the alarm flags are checked. Where the note meets these tests, the note approval light is illuminated. Where a note fails one of the tests, a note alarm light is illuminated and the system activates the video surveillance system to record evidence of the person passing the note. The actual process used in this case will vary depending on the threat and safety profile of the end user.

The software in the terminal unit may be embedded within a Read Only Memory (ROM). The software is preferably written in a 4GL language and compiled prior to the burning of a ROM. This is to allow customisation of the software for each particular site. The software is used to determine the denomination of the note through colour analysis and the structure of all other features/indicia scanned. Once the scan is completed, the image file is processed to retrieve the note number and a colour profile number is generated.

In a third embodiment, portable wallets are designed to

enable the safe transit of cash or securities.

The wallet will record the serial number data onto a small retrieval card, as the cash is scanned as it enters a storage receptacle.

The card will be required to either deposit or retrieve notes from the wallet. This will enable the safe transit and storage of the wallet.

In a fourth embodiment, a small lipstick sized, portable, rechargeable scanning wand enables designated cash notes to be scanned, for instance, in the hotel room before going out shopping. The serial numbers of the scanning notes are stored in the wand. If cash (or the wallet) is stolen, the wand has a record of the stolen note(s).

An add-on or integrated system associated with a mobile phone may be used to allow notes to be cleared at a remote location (eg., purchasing a car on the week-end with cash).

The database for currency/bank notes is established as follows:

Notes are scanned into the system at the Mint. The number and any microdot (or other) security patterns are confirmed and stored as a new masterfile and finally a master note image is recorded. From this master image, a reference colour is set and

captured.

All legitimate serial numbers of all notes and denominations that have been issued by the Mint are on the database.

If a scanned serial number does not match with a serial number legitimately issued by the Mint, an alarm will be sent to the terminal unit via a light or other type of silent alarm.

If a note is presented to the system that creates an image file outside the tolerances of acceptability, the serial number or the masterfile will be marked and the note will be withdrawn from circulation when presented at a banking interface.

The system will allow the banks to automatically separate the worn, torn damaged and incomplete notes.

It is envisaged that new types of notes will be created to incorporate new colour encryption devices, colour encrypted watermarks, and microdot colour patterns through 16.7 million colours each tied to the serial number. This mark will, in turn, be able to be used to independently verify the validity of the note offline.

In line with new technologies, the clear hologram window can be used to verify the unique polymer colour to add to the overall analysis of the note. This will mean that any particular note will be able to be independently verified with a number of different and independent tests.

Forging of the note will require:

a) knowledge of the colour serial number link;

b) knowledge of the encrypted watermark;

c) the use of the correct polymer blend;

d) a valid serial number from the Mint.

Cheques can have a colour dot serial number link and a link to the signature. The cheque can also, using this feature, have a unique PIN (personal identification number), which will allow the instant authorisation of the cheque.

For ultra secure company cheques, the cheques can be made up at the company and specially printed with a microdot pattern that gives an audit trail in the company to the process used to draw the cheque. This will allow cheques to be made up on demand and the machine can code all of the information into the cheque pattern prior to issue.

Another device that can be used to secure the cheque and can be used for travellers cheques is a thumbprint. This print pad can be a polymer that dries quickly when exposed to air. When the cheque is used, the top is peeled off the square and the print made. Within a very short time, the print dries and the cheque is presented. The scanner detects the image and compares it against a file entry of allowable prints.

Thumb cheques do not require a signature. It is hard to

forge a fingerprint and the person who signs the cheque is secret and no name needs to be on the cheque. The cheque can be authorised upon presentation to the bank or other financial institution. Security devices can be built into the cheque and if a person is made to validate the cheque under duress, a duress fingerprint can be used. Th system will be able to recognise the duress alarm and activate the security procedures.

Signatures can be unreliable, for instance, after injury or with Parkinsons Syndrome. Using the system, a validated signature file can be automatically updated. Validation can use a mixture of personal verification and advanced software tools such as fractals and chaos analysis.

Travellers cheques can have serial number and PIN identification, and can also incorporate a duress PIN feature and/or can use the polymer thumbprint devices. A PIN signature can be digitally encrypted into the travellers cheque. Stolen cheques can be easily traced and dishonoured.

The system prevents business from:

1. Theft.

All notes stored on the business premises, as scanned, will be on file. If robbed, the owner only needs to press an alarm code and the details of all of the notes on file are transmitted to the security section of the system and marked immediately as stolen.

This information is then passed to all of the relevant authorities.

2. Misappropriation.

All scanned notes can be put into a database and the business owner knows with confidence the amount of cash flow through the business in relation to stock held or sold.

3. Theft/Misuse of Cheques (Personal and Travellers).

A client is requested, upon opening an account at a financial institution, to supply:

a) A PIN (personally selected);

b) Signature;

c) Finger prints - (i) designated finger for approval; and (ii) designated finger for alarm.

d) Usual identification documentation.

The PIN, signature and fingerprints are all ditigized and stored in the secure database. Whenever a cheque is presented to a terminal, the relevant sections of the captured image are analysed and compared to the master files in the relevant databases (eg., fingerprint and signature databases).

In addition, a secure PIN number may be entered into the terminal allowing instant cheque clearance, much like current plastic credit cards.

An additional feature of the EFTPOS type terminal could include a small digitizer pad for fingerprint authentication. This could

either replace the current PIN number authentication or be used as an added layer of security.

Digital signature comparison to master files could be included which compares the signature on the credit card with the master file signature as well as comparison with the client created signature at the site of cash dispersal.

All inconclusive results will be referred to a central service centre for attention.

Databases (with ongoing upgrade) can store the following information:

a) valid note files - include image and serial numbers;

b) valid note serial numbers;

c) stolen/missing note registry (NB: a drug dealer who obtains his cash from various drug dealers could potentially be apprehended as he deposits the cash into his/her account, as much of the cash will probably have been stolen in armed robberies, etc.);

d) destroyed note registry;

e) damaged note registry (notes earmarked for removal and destruction);

f) fingerprint digitized image files;

g) signature digitized image files;

h) PIN number client registry.

System uses include:

a) security - all notes scanned into the system, whether in the till, a cash box, safe or wallet, etc.;

b) counterfeit detection;

c) damaged note detection;

d) identification of money laundering and other illegal currency transactions (once the system comes into general use, individual notes can be tracked).

The proposed system (in one or more embodiments) is designed to enable one or more of the following;

1. Cash, personal cheques and travellers cheques to be assessed for authenticity at the point of presentation.

2. Cash notes, serial numbers and computer image files to be stored at secure national processing laboratory in addition to a central international centre.

3. Cash serial numbers, which enter the system, are compared to master files of authentic serial numbers supplied by the national Mint.

4. Cash serial numbers, which enter the system, are compared to master files of stolen note serial numbers.

5. Cash serial numbers, which enter the system, are compared to other note serial numbers currently stored within the system to see if any duplications are present.

6. Recording and deleting of note serial numbers as

they enter and leave the till at the end user interface. This allows a digital record of cash transactions going through the till, in addition to recording the serial numbers of notes held within the till should a thief occur.

7. Colour and image analysis of presented tender, identifying damaged notes which are then recorded centrally and digitally tagged to allow their removal from circulation at an appropriate location.

8. Appropriate law enforcement agencies to be notified of any stolen or forged notes presented to the system or any notes stolen from the system.

9. Integration of the system into secure tills, secure cash transportation boxes and safes.

10. Remote cash authentication using either a conventional mobile phone with a specifically designed clip-on scanner, or an integrated mobile phone with built-in scanner. Customers can dial into the national centre, enter a PIN number and then scan the notes at the point of sale.

11. Option of small, lipstick sized optical scanner, which can be manually rolled over the serial number on a cash note. This serial number is compared to stored numbers within the ROM within the device. The device is battery powered and the ROM is upgradeable.

12. The tracking of individual notes as they move throughout the market (once the system has been fully implemented within a nation).

13. Integrated internationally operation centre will notify other national centres and law enforcement agencies (eg., FBI) of stolen or forged foreign currency and notes.

14. Personal and travellers cheques can be cleared by using a personal PIN number as well as a signature upon presentation to the system.

15. Personal cheques presented to the system can be electronically checked against account balances (in a similar fashion to plastic cash cards).

16. Clients' signatures and/or finger prints can be scanned into the system when an account is opened at a financial institution. This maser signature file can then be compared against signatures and/or finger print admitted to the system at a later date upon cheque presentation.

17. Special cheques to be manufactured, which allow a finger print to be placed on the cheque in place of or in addition to a signature. A region of the cheque can have a peel of polymer cover which reveals a polymer pad which enables a fingerprint to be made. The polymer pad solidifies a few seconds after the peel off cover has been removed. Customers can designate the finger they wish to use

and can include an alarm finger. Fingerprints allow a degree of anonymity and allow disabled people (eg., Parkinsonism, etc.) to avoid the signature process.

18. Photocopiers where "secure" documents having identifying features/indicia can only be copied by authorised persons.

It will be readily apparent to the skilled addressee that the range of potential applications is limitless.

Various changes and modifications may be made to the embodiments described and illustrated without departing from the present invention.

DATED this eighth day of September 1999.

ACCUDENT PTY LTD

By its Patent Attorneys

FISHER ADAMS KELLY

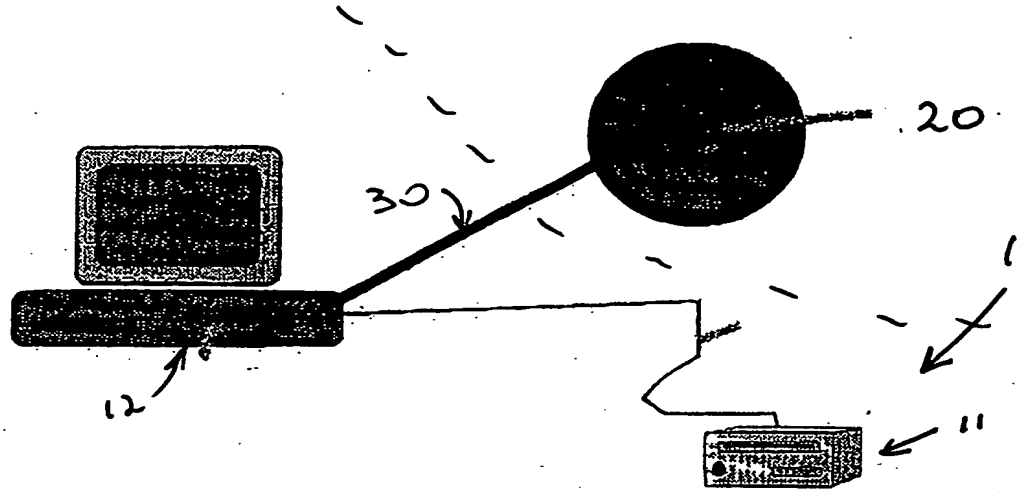


Fig.1

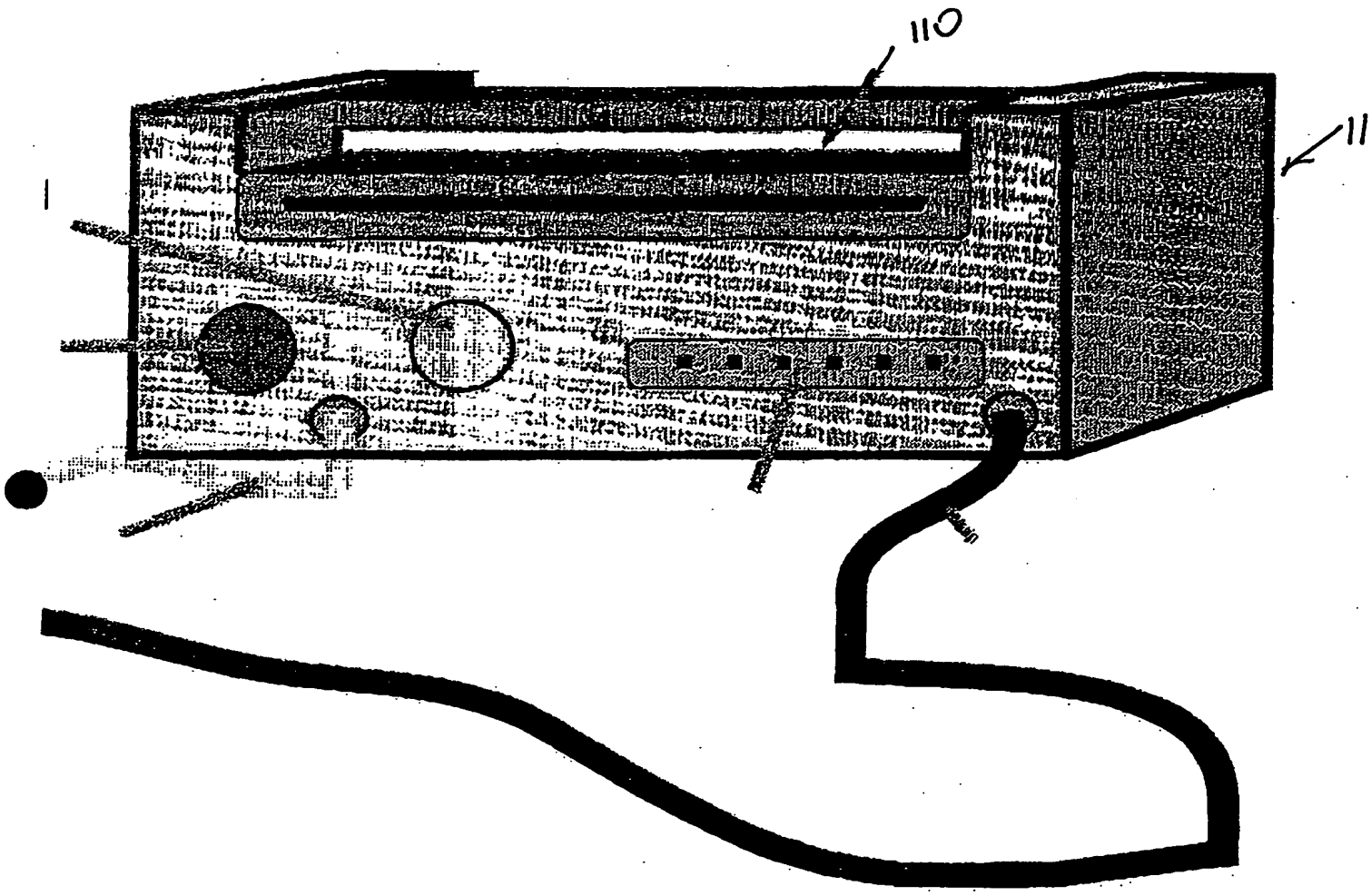


Fig.2